



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,974	12/05/2001	Royce E. Slick	36.P327	9396

5514 7590 02/01/2007
FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER

CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
----------	--------------

2136

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 10/010,974	Applicant(s) SLICK ET AL.	
	Examiner David G. Cervetti	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 November 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5 and 7-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5 and 7-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 October 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Applicant's arguments filed November 17, 2006, have been fully considered but they are not persuasive.
2. Claims 1-5 and 7-27 are pending and have been examined. Claims 6 and 28-34 have been cancelled.

Response to Amendment

3. The objection of claim 12 and 24-26 is withdrawn.
4. The rejection of claims 1, 22-23, 27-28, and 31 under 35 U.S.C. 112, second paragraph, is withdrawn.
5. Applicant's arguments with respect to the prior art have been considered but are moot in view of the new ground(s) of rejection.
6. **The applicant has not traversed the examiner's use of official notice with regards to the claimed limitations found in claims 2, 9, and 15, these features are taken by the examiner to be admitted prior art since the applicant has not adequately challenged the examiner's use of official notice (see MPEP 2144.03(c), 2144.04).**

Claim Rejections - 35 USC § 103

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
8. Claims 1-5 and 7-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Otway et al. (US Patent 7,020,773, hereinafter Otway), and further in view of and Lapstun et al. (US Patent 7,062,651, hereinafter Lapstun).

Regarding claims 1 and 27, Otway teaches

- a method for securely storing a public key for encryption of data in a computing device, the method using a user-specific key pair which is securely stored in the computing device (**abstract, col. 3, lines 54-67, col. 4, lines 1-5**), the method comprising:
- a user authenticating step of authenticating a user who logs into the computing device (**col. 3, lines 54-67, col. 4, lines 1-5**);
- a registering step of registering the user-specific key pair of the user authenticated by said authenticating step, wherein the user-specific key pair is registered in a secure registry (**col. 3, lines 54-67, col. 4, lines 1-5**);
- a receiving step of receiving a target public key corresponding to a target device (**col. 2, lines 30-60**);
- an obtaining step of obtaining the user-specific key pair from the secure registry (**col. 2, lines 48-67**);
- a key encrypting step of using a user-specific private key from the user-specific key pair to create a target key verifier based on the target public key (**col. 2, lines 48-67**);
- a storing step of storing the target key verifier and the target public key in a storage area (**col. 2, lines 59-67, col. 3, lines 1-30**);
- a retrieving step of retrieving the target key verifier and the target public key from the storage area (**col. 2, lines 59-67, col. 3, lines 1-30**);

- a verification step of applying a user-specific public key from the user-specific key pair to the target key verifier for verifying the authenticity of the target public key, wherein said verification step verifies whether the public key in the storage area and the public key in the secure registry correspond to each other (**col. 3, lines 30-67**); and
- a data encrypting step of encrypting data with the target public key, in the case that the authenticity of the target public key is verified, thereby creating encrypted data for transmission to the target device (**col. 4, lines 19-55**).

Otway does not expressly disclose using it for printing purposes. However, Lapstun teaches registering a printer and providing a printer with a key pair for authentication and encryption purposes and a recognizing step of recognizing a printing instruction (**col. 31, lines 20-67**). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the mutual authentication schemes of Otway with the secure, authenticated printer of Lapstun. One of ordinary skill in the art would have been motivated to do so to ensure that the client sends printing data to an authenticated/trusted printer and that the printer receives data from an authenticated/trusted client (**Lapstun, col. 30, lines 50-67, col. 31, lines 1-67, col. 32, lines 1-20**).

Regarding claim 22, Otway teaches

- a method for securely storing a printer public key for encryption of print data in a computing device, the method using a user-specific key pair

which is securely stored in the computing device (**abstract, col. 3, lines 54-67, col. 4, lines 1-5**), the method comprising:

- a user authenticating step of authenticating a user who logs into the computing device (**col. 3, lines 54-67, col. 4, lines 1-5**);
- a registering step of registering the user-specific key pair of the user authenticated by said authenticating step, wherein the user-specific key pair is registered in a secure registry (**col. 3, lines 54-67, col. 4, lines 1-5**);
- a receiving step of receiving a public key (**col. 2, lines 30-60**);
- an obtaining step of obtaining a user-specific key pair from a secure registry upon receipt of a corresponding user identification (**col. 2, lines 48-67**);
- a first hashing step of applying a hashing algorithm to the public key to create a first key hash (**col. 2, lines 48-67**);
- an encryption step of applying an encryption algorithm to encrypt the first key hash with a user-specific private key from the user-specific key pair, thereby creating a key signature (**col. 2, lines 30-60**);
- a storing step of storing the key signature and the public key in a storage area (**col. 2, lines 30-60**);
- a retrieving step of retrieving the key signature and the public key from the storage area (**col. 2, lines 30-60**);

- a second hashing step of applying the hashing algorithm to the retrieved public key to create a second key hash (**col. 2, lines 30-60**);
- a decrypting step of applying a decryption algorithm to decrypt the key signature with a user-specific public key from the user-specific key pair, thereby retrieving the first key hash (**col. 2, lines 30-67**);
- a verification step of applying a verification algorithm to compare the first printer key hash with the second printer key hash, for verifying the authenticity of the retrieved printer public key, wherein said verification step verifies whether the public key in the storage area and the public key in the secure registry correspond to each other (**col. 3, lines 30-67**);
and
- a data encrypting step of applying an encryption algorithm to data using the retrieved public key, in the case that the authenticity of the retrieved public key is verified, to create encrypted data for transmission (**col. 4, lines 19-55**).

Otway does not expressly disclose using it for printing purposes. However, Lapstun teaches registering a printer and providing a printer with a key pair for authentication and encryption purposes and a recognizing step of recognizing a printing instruction (**col. 31, lines 20-67**). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the mutual authentication schemes of Otway with the secure, authenticated printer of Lapstun. One of ordinary skill in the art would have been motivated to do so to ensure that the client

Art Unit: 2136

sends printing data to an authenticated/trusted printer and that the printer receives data from an authenticated/trusted client (**Lapstun, col. 30, lines 50-67, col. 31, lines 1-67, col. 32, lines 1-20**).

Regarding claim 23, Otway teaches

- a method for authentication of a public key received by a computing device, the method comprising:
- a user authenticating step of authenticating a user who logs into the computing device (**abstract, col. 3, lines 54-67, col. 4, lines 1-5**);
- a registering step of registering the user-specific key pair of the user authenticated by said authenticating step, wherein the user-specific key pair is registered in a secure registry (**col. 3, lines 54-67, col. 4, lines 1-5**);
- a first receiving step of receiving in the computing device a public key corresponding to a printer (**col. 2, lines 30-60**);
- a hashing step of applying a hashing algorithm to the public key to create a first key hash (**col. 2, lines 48-67**);
- a second receiving step of receiving in the computing device a predetermined second key hash obtained from a test page printed by the printer, wherein the second key hash is input into the computing device by a user-input means connected to the computing device (**col. 3, lines 1-30, col. 5, lines 20-60**);

- a verification step of applying, in response to recognizing the printing instruction, a verification algorithm to compare the first printer key hash with the second printer key hash, for verifying the authenticity of the received printer public key, wherein said verification step verifies whether the public key in the storage area and the public key in the secure registry correspond to each other (**col. 3, lines 30-67**); and
- a storing step of storing, in the case that the authenticity of the received printer public key is verified in the verification step, the received printer public key in a memory area of the computing device (**col. 2, lines 30-60**).

Otway does not expressly disclose using it for printing purposes. However, Lapstun teaches registering a printer and providing a printer with a key pair for authentication and encryption purposes and a recognizing step of recognizing a printing instruction (**col. 31, lines 20-67**). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the mutual authentication schemes of Otway with the secure, authenticated printer of Lapstun. One of ordinary skill in the art would have been motivated to do so to ensure that the client sends printing data to an authenticated/trusted printer and that the printer receives data from an authenticated/trusted client (**Lapstun, col. 30, lines 50-67, col. 31, lines 1-67, col. 32, lines 1-20**).

Regarding claim 2, the combination of Otway and Lapstun teaches wherein the user-specific key pair is obtained from a key function call which is supported by an

operating system executing in the computing device (**Otway, fig. 1, col. 1, lines 40-67**) and these features have been admitted per applicant to have been conventional and well known to digital rights management systems at the time the invention was made.

Regarding claim 3, the combination of Otway and Lapstun teaches wherein the operating system securely maintains a user-specific key pair for each of a plurality of users of the computing device (**col. 3, lines 54-67, col. 4, lines 1-5**).

Regarding claim 4, the combination of Otway and Lapstun teaches wherein each user-specific key pair can only be accessed by providing the operating system with user identification data corresponding to the user-specific key pair (**col. 3, lines 54-67, col. 4, lines 1-5**).

Regarding claim 5, the combination of Otway and Lapstun teaches wherein the target key verifier created in the key encrypting step is an encrypted version of the target public key (**col. 4, lines 32-67**).

Regarding claim 7, the combination of Otway and Lapstun teaches wherein the verification step includes decrypting the target key verifier with the user-specific public key using a decryption algorithm (**col. 4, lines 32-67**).

Regarding claim 8, the combination of Otway and Lapstun teaches wherein the verification step further includes using a key verification algorithm to compare the decrypted target key verifier to the target public key for verifying the authenticity of the target public key (**col. 5, lines 1-20**).

Regarding claim 9, the combination of Otway and Lapstun teaches wherein the verification step is performed by a verification function call which is supported by an

Art Unit: 2136

operating system executing in the computing device (**Otway, fig. 1, col. 1, lines 40-67**) and these features have been admitted per applicant to have been conventional and well known to digital rights management systems at the time the invention was made.

Regarding claim 10, the combination of Otway and Lapstun teaches wherein the target key verifier created in the key encrypting step is a digital signature of the target public key (**Lapstun, col. 2, lines 1-32**).

Regarding claim 11, the combination of Otway and Lapstun teaches wherein the digital signature of the target public key is created by applying a hashing algorithm to the target public key to obtain a target key hash, and then encrypting the target key hash with the user-specific private key using an encryption algorithm (**Lapstun, col. 2, lines 1-32**).

Regarding claim 12, the combination of Otway and Lapstun teaches wherein the digital signature of the target public key is created by applying a hashing algorithm to the target public key to obtain a target key hash, and then subjecting the target key hash to an encryption algorithm (**Lapstun, col. 2, lines 1-32**).

Regarding claim 13, the combination of Otway and Lapstun teaches wherein the verification step includes decrypting the target key verifier with the user-specific public key using a decryption algorithm to obtain a decrypted target key hash (**Lapstun, col. 2, lines 1-32**).

Regarding claim 14, the combination of Otway and Lapstun teaches wherein the verification step further includes reapplying a hashing algorithm to the target public key to obtain a new target key hash and using a hash verification algorithm to compare

Art Unit: 2136

the decrypted target key hash to the new target key hash for verifying the authenticity of the target public key (**Lapstun, col. 2, lines 1-32**).

Regarding claim 15, the combination of Otway and Lapstun teaches wherein the verification step is performed by a verification function call which is supported by an operating system executing in the computing device (**Otway, fig. 1, col. 1, lines 40-67**) and these features have been admitted per applicant to have been conventional and well known to digital rights management systems at the time the invention was made.

Regarding claim 16, the combination of Otway and Lapstun teaches wherein the receiving step includes applying a hashing algorithm to the received target public key to obtain a received target key hash and using a hash verification algorithm to compare the received target key hash to a test target key hash for verifying the authenticity of the received target public key (**Otway, col. 2, lines 48-67, Lapstun, col. 2, lines 1-32**).

Regarding claim 17, the combination of Otway and Lapstun teaches wherein the test target key hash is input by a user (**Otway, col. 5, lines 20-60**).

Regarding claim 18, the combination of Otway and Lapstun teaches wherein the target device is a printer and wherein the test target key hash is obtained from a test page printed by the printer (**Otway, col. 5, lines 20-60, Lapstun, col. 31, lines 20-67**).

Regarding claim 19, the combination of Otway and Lapstun teaches wherein the target device is a printer and the target public key is a printer public key (**Lapstun, col. 31, lines 20-67**).

Regarding claim 20, the combination of Otway and Lapstun teaches wherein, in the receiving step, the printer public key is received in response to a key request sent to the printer (**Lapstun, col. 31, lines 20-67**).

Regarding claim 21, the combination of Otway and Lapstun teaches wherein the method is performed in a printer driver executing on the computing device (**Lapstun, col. 31, lines 20-67**).

Regarding claim 24, the combination of Otway and Lapstun teaches a computing device for authenticating a public key for encryption of data, said computing device comprising: a program memory for storing process steps executable to perform a method according to any of Claims 1 to 23; and a processor for executing the process steps stored in said program memory (**abstract**).

Regarding claim 25, the combination of Otway and Lapstun teaches computer-executable process steps stored on a computer readable medium, said computer-executable process steps for authenticating a public key for encryption of data, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 23 (**abstract**).

Regarding claim 26, the combination of Otway and Lapstun teaches a computer-readable medium which stores computer-executable process steps, the computer-executable process steps to authenticate a public key for encryption of data, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 23 (**abstract**).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. **Lee (US Patent 6,628,413)** teaches a JAVA printer using any available security technique (columns 3-6). **Lloyd (US Patent Application Publication 2003/0014640)** teaches a printer using public key encryption and hash functions to verify information in transit has not been tampered with (paragraphs 20-30). **Wu et al. (US Patent Application Publication 2002/0042884)** teaches a printer, digital certificate, hash functions, and public key encryption for providing a secure printing environment, authenticating a printer, etc. (pages 7-13). **Takaragi et al. (US Patent 6,370,247)** teaches using hash values and encryption for data protection (columns 5-6). **Fischer (US Patent 5,005,200)** teaches a public key/digital signature system. **Debry (US Patent 6,918,042)** teaches a printer storing a key and a certificate authority also storing said key.

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.


11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

12. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

13. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DGC

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


1/31/07